UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/600,683	06/20/2003	Erik Olson	13768.373	4994

47973   7590   05/24/2007
WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER
WILLIAMS, JEFFERY L

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
05/24/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/600,683	OLSON ET AL.
	Examiner	Art Unit
	Jeffery Williams	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>14 March 2007</u>.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1 – 12, 14 – 22, 24 – 29</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1 – 12, 14 – 22, 24 – 29</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

1   **DETAILED ACTION**

2

3   Claims 1 – 12, 14 – 22, 24 – 29 are pending.

4   All objections and rejections not set forth below have been withdrawn.

5

6   ***Specification***

7

8   The specification is objected to as failing to provide proper antecedent basis for

9   the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction

10   of the following is required:

11   Amendments to claims 1 – 12, 14 – 22, 24 – 29 add new recitations substantially

12   comprising: *"the request includes a first portion of safe data, and a second portion of*

13   *data"* , *"wherein the HTTP request includes a safe portion and a user input portion that*

14   *includes data that was not generated by the server computer "*, *"refraining from serving*

15   *a response to any portion of the request if..."*, *"refusing to dynamically render a*

16   *response to any portion of the HTTP request"*, and *"evaluating only the second portion*

17   *of the request"*. The specification fails to provide proper antecedent basis for these

18   recitations.

19

1   *Claim Objections*

2

3   Claim 8 is objected to because of the following informalities: A comma should

4   precede the clause "if the input data includes a script construct", as it is presumed that

5   the applicant wishes for this conditional to modify the action of refusing to render a

6   response. Appropriate correction is required.

7

8

9   *Claim Rejections - 35 USC § 112*

10

11   **The following is a quotation of the first paragraph of 35 U.S.C. 112:**

12   The specification shall contain a written description of the invention, and of the manner and process of
13   making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the
14   art to which it pertains, or with which it is most nearly connected, to make and use the same and shall
15   set forth the best mode contemplated by the inventor of carrying out his invention.
16
17   **Claims 1 – 12, 14 – 22, 24 – 29 are rejected under 35 U.S.C. 112, first**

18   **paragraph, as failing to comply with the written description requirement.** The

19   claim(s) contains subject matter which was not described in the specification in such a

20   way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the

21   time the application was filed, had possession of the claimed invention. Applicant has

22   not pointed out where the new (or amended) claim is supported, nor does there appear

23   to be a written description of the claim limitations in the application as filed (see above

24   objection to the specification).

25
26

1   The following is a quotation of the second paragraph of 35 U.S.C. 112:

2   The specification shall conclude with one or more claims particularly pointing out and distinctly
3   claiming the subject matter which the applicant regards as his invention.
4
5   **Claims 1 – 12, 14 – 22, 24 – 29 are rejected under 35 U.S.C. 112, second**

6   **paragraph, as being indefinite for failing to particularly point out and distinctly**

7   **claim the subject matter which applicant regards as the invention.**

8   Specifically, claims 1, 8, and 18, each comprise the limitation (or essentially

9   similar), *"refraining from serving a response to any portion of the request"*. However,

10   the examiner notes that the applicant, in contradiction, subsequently claims (see claims

11   1, 7, 8, 18) that the server computer, in response to a portion of a request, serves an

12   error response to the client. Accordingly, these recitations render the scope of these

13   claims unclear.

14   Depending claims are rejected by virtue of dependency.

15

16   *Claim Rejections - 35 USC § 103*

17

18   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

19   obviousness rejections set forth in this Office action:

20   (a) A patent may not be obtained though the invention is not identically disclosed or described as set
21   forth in section 102 of this title, if the differences between the subject matter sought to be patented and
22   the prior art are such that the subject matter as a whole would have been obvious at the time the
23   invention was made to a person having ordinary skill in the art to which said subject matter pertains.
24   Patentability shall not be negatived by the manner in which the invention was made.
25
26   **Claims 1 – 12, 14 – 22, 24 – 29 are rejected under 35 U.S.C. 103(a) as being**

27   **unpatentable over CERT CC, "CERT Advisory CA-2000-02 Malicious HTML Tags**

28   **Embedded in Client Web Requests" (CERT-Advisory) in view of CERT CC,**

1   **"Understanding Malicious Content Mitigation for Web Developers" (CERT) in view**

2   **of Wheeler, <u>Secure Programming for Linux and Unix HOWTO</u> in view of Sanin,**

3   **"Web Service Security Filter", U.S. Patent Publication 2004/0073811.**

4

5   Regarding claim 1, CERT-Advisory discloses:

6   *receiving a request from a user computer, wherein the request includes a first*

7   *portion of safe data, and a second portion of data derived from an outside source*

8   (CERT-Advisory, page 1, Systems Affected, Overview; page 2, pars. 2-4).

9   CERT-Advisory discloses, in general, that the Server site attempts to prevent the

10   site from being abused or attacked by malicious data ("a marker of active content")

11   within the request (CERT-Advisory, page 5, Solutions for Web Page Developers and

12   Web Site Administrators). CERT-Advisory does not *explicitly* say *determining if the*

13   *request from the user computer includes a marker of active content identified in a list of*

14   *active markers.* Instead, CERT-Advisory directs the readers' attention to the detailed

15   solution (found in CERT) for preventing cross-site scripting attacks in response to

16   receiving HTTP requests comprising malicious scripts.

17   CERT discloses the specifics for mitigating cross-site scripting attacks by

18   evaluating the incoming data requests against a list of markers of active content that

19   woud indicate the presence of malicious scripts (CERT, page 1, par. 1, Problem

20   Summary, pars. 2-3; page 2, Mitigation Summary; page 3, Identifying the Special

21   Characters; pages 4 and 5, Filtering Dynamic Content).

1   It would have been obvious to one of ordinary skill in the art to combine the

2   teachings of CERT with the teachings of CERT-Advisory. This would have been

3   obvious because CERT-Advisory explicitly says to include the reference of CERT so as

4   to successfully mitigate cross-site scripting attacks (CERT-Advisory, page 5, par. 6).

5   The combination of CERT-Advisory and CERT discloses *refraining from serving*

6   *a response to a portion of the request if the request includes the marker of active*

7   *content to dynamically render a response to the HTTP request if the input data includes*

8   *a script construct* (CERT-Advisory, pg. 1, "Overview"; pg. 2, "Malicious code sent

9   inadvertently by a client for itself"; CERT, pg. 1, par. 1; pg. 2-4, "Mitigation Summary").

10 Herein, prior art discloses that if the input data includes a script construct, refusing to

11 execute HTTP request and thereby preventing the cross-site scripting attack if the input

12 data includes a script construct. Malicious HTTP requests are not executed.

13   The combination does not disclose *informing the user that a marker of active*

14 *content from the list of active markers has been discovered in the request and*

15 *requesting that the user computer resubmit a request and subsequently serving a*

16 *response to the request resubmitted by the user computer..*

17   Wheeler, in response to the problem of cross-site scripting attacks and building

18 upon the prior art teachings of CERT (Wheeler, 4.10, 6.15, 6.15.1 – 6.15.2.1, 8.5),

19 teaches that a system in practice may forbid markers of active content and send

20 informative error messages to users who include them in requests. A system could

21 notify the user of ways to correct such issues (Wheeler, 4.11.6, par. 2; 4.11.1; 4.11.3,

22 par. 5; 4.12, par. 5).

1   It would have been obvious to one of ordinary skill in the art to employ the

2   teachings of Wheeler along with the teachings of the combination of CERT and CERT-

3   Advisory. This would have been obvious because one of ordinary skill in the art would

4   have been motivated by the explicit suggestions found within the prior art when

5   practically implementing a solution to mitigate malicious scripting attacks.

6   The examiner notes that the applicant adds the following recitation, which does

7   not appear to be explicitly recited within the prior art combination. Namely, the

8   combination does not appear to explicitly recite maintaining the list of active markers *"at*

9   *a server"*.

10   Sanin, however, discloses that a list of active markers should be maintained at a

11   server (fig. 1:102), thus allowing a server to continually protect itself with an updated list

12   that reflects newly discovered types of web attacks (par. 16). Sanin discloses that his

13   method of protection against cross site scripting attacks is an enhancement to the

14   known prior art methods of request validation and/or encoding, as disclosed within the

15   prior art combination (par. 14, 15). One of ordinary skill in the art would have been

16   motivated to employ the teachings of Sanin within the combination, as one of ordinary

17   skill in the art would have been motivated by Sanin's teachings of an enhancement.

18   Furthermore the combination enables:

19   refraining from serving a response to *any portion* of the request (Sanin, par. 38,

20   39; Wheeler, 4.11.6, par. 2; 4.11.1; 4.11.3, par. 5; 4.12, par. 5).

21

1   Regarding claim 8, it comprises substantially the same limitations as claim 1, and

2   it is rejected, at least, for the same reasons.

3

4   Regarding claim 9, the combination disclose:

5   *at least one of: receiving a query string that includes at least one query string*

6   *variable; receiving a cookie; receiving one or more headers in the HTTP request; and*

7   *receiving one or more form fields* (CERT-Advisory, page 2, pars. 2-5; CERT, page 2,

8   Mitigation Summary).

9

10   Regarding claim 10, the combination disclose:

11   *at least one of: searching the HTTP request for one or more character*

12   *combinations that correspond to a script construct; searching the HTTP request for an*

13   *event that includes a script construct; searching server variables that derive input data*

14   *from another source; and searching the HTTP request for an expression that includes a*

15   *script construct* (CERT, page 3, Identifying the Special Characters; page 4, Filtering

16   Dynamic Content).

17

18   Regarding claim 11, the combination disclose:

19   *searching the input data for a script construct* (CERT, page 3, Identifying the

20   Special Characters; page 4, Filtering Dynamic Content).

21

22   Regarding claim 12, the combination disclose:

1   *searching for patterns associated with scripts* (CERT, page 3, Identifying the

2   Special Characters; page 4, Filtering Dynamic Content).

3

4   Regarding claim 14, the combination disclose:

5   *wherein preventing the cross-site scripting attack if the input data includes a*

6   *script construct further comprises logging an event at the server computer* (Wheeler,

7   8.1; 10.9; 10.11). Herein, the combination disclose that a server generates a detailed

8   log of events regarding system successes and failures, in addition to sending a

9   response back to the user regarding the event – such as why there was a failure.

10

11   Regarding claim 15, the combination of CERT-Advisory, CERT, Hidalgo, and

12   Fielding disclose:

13   *encoding the user input including the script construct to render the script inert*

14   (CERT-Advisory, page 2, par. 1; page 5, pars. 3-6; CERT, page 3, Identifying the

15   Special Characters; page 4, par. 2).

16

17   Regarding claim 16, the combination of CERT-Advisory, CERT, Hidalgo, and

18   Fielding disclose:

19   *evaluating the HTTP request to determine in the input data includes a marker of*

20   *active content* (CERT, page 2, Mitigation Summary – particularly steps 2 and 4; page 3,

21   Identifying the Special Characters).

22

1   Regarding claim 17, the combination of CERT-Advisory, CERT, Hidalgo, and

2   Fielding disclose:

3   *determining if the marker of active content is within a particular element, wherein*

4   *the marker of active content is harmful only when rendered within the particular element*

5   (CERT, page 2, Mitigation Summary – particularly steps 2 and 4 (identifying special

6   characters, filtering specific characters in dynamic elements; page 3, Identifying the

7   Special Characters).

8

9   Regarding claims 2 – 3, 5 – 7, 18 – 22, 24, and 25, they are method and method

10   embodied on computer readable medium claims corresponding to the system claims 1 –

11   17, and they are rejected, at least, for the same reasons.

12

13   Regarding claim 4, the combination enables: *evaluating only the second portion*

14   *of the request that includes the data derived from an outside source* (CERT, page 2,

15   Mitigation Summary; Wheeler, sect. 4, par. 1, 12). The combination enables the need

16   to evaluate data comprising untrusted input that could be transmitted in an HTTP

17   request.

18

19   Regarding claim 26, the combination enables:

20   *wherein determining if the request from the user computer includes a marker of*

21   *active content comprises evaluating only user input fields of the request* (CERT, page 2,

22   Mitigation Summary; Wheeler, sect. 4, par. 1, 12). The combination enables the need

1   to only evaluate data comprising untrusted input that could be transmitted in an HTTP

2   request.

3

4   Regarding claim 27, the combination enables maintaining a "highly customizable"

5   list of markers of active content (Cert, pg. 4, 5; Sanin, par. 16) including *inactivating*

6   *markers in the list of markers* (Sanin, table 4).

7

8   Regarding claim 28, the combination enables:

9   *wherein evaluating the HTTP request to determine if the input data includes a*

10   *script construct comprises evaluating the HTTP request for an event* (Wheeler, sect.

11   4.11.3, box of attack types). Herein, the combination teaches to test for events, such as

12   'onmousover' events. It does not disclose onclick events, however, one of ordinary skill

13   in the art would have recognized that an 'onclick' events similarly introduce scripts such

14   as 'onmouseover' events (applicant may refer to evidence such as W3C

15   Recommendation, "Scripts") and would have been motivated to test for malicious

16   constructs.

17

18   Regarding claim 29, the combination discloses:

19   wherein evaluating the HTTP request to determine if the input data includes a

20   script construct comprises evaluating the HTTP request for an element size expression

21   (Wheeler, sect. 4.11.3, box of attack types).

1

2   ***Response to Arguments***

3

4   Applicant's arguments with respect to claims 1 - 29 have been considered but are

5   moot in view of the new ground(s) of rejection.

6

7   ***Conclusion***

8

9   The prior art made of record and not relied upon is considered pertinent to

10   applicant's disclosure:

11

12   ***See Notice of References Cited***

13

14   A shortened statutory period for reply to this final action is set to expire THREE

15   MONTHS from the mailing date of this action. In the event a first reply is filed within

16   TWO MONTHS of the mailing date of this final action and the advisory action is not

17   mailed until after the end of the THREE-MONTH shortened statutory period, then the

18   shortened statutory period will expire on the date the advisory action is mailed, and any

19   extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

20   the advisory action. In no event, however, will the statutory period for reply expire later

21   than SIX MONTHS from the date of this final action.

1   Any inquiry concerning this communication or earlier communications from the

2   examiner should be directed to Jeffery Williams whose telephone number is (571) 272-

3   7965. The examiner can normally be reached on 8:30-5:00.

4   If attempts to reach the examiner by telephone are unsuccessful, the examiner's

5   supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

6   number for the organization where this application or proceeding is assigned is 571-

7   273-8300.

8   Information regarding the status of an application may be obtained from the

9   Patent Application Information Retrieval (PAIR) system. Status information for

10 published applications may be obtained from either Private PAIR or Public PAIR.

11 Status information for unpublished applications is available through Private PAIR only.

12 For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

13 you have questions on access to the Private PAIR system, contact the Electronic

14 Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

15 USPTO Customer Service Representative or access to the automated information

16 system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

17

18
19 J. Williams
20 AU: 2137
21 ᴣᴡ

22

                                   EMMANUEL L. MOISE
                                   SUPERVISORY PATENT EXAMINER